IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of :

Takashi YUMIBA et al. :

Serial No. NEW : **Attn: Application Branch**

Filed September 26, 2000 : **Attorney Docket No. 2000_1253A**

#4

INFORMATION RECORDING MEDIUM FOR RECORDING A SCRAMBLED PART OF CONTENT INFORMATION, AND METHOD AND APPARATUS FOR REPRODUCING INFORMATION RECORDED THEREIN

CLAIM OF PRIORITY UNDER 35 USC 119

Assistant Commissioner for Patents
Washington, DC 20231

Sir:

Applicants in the above-entitled application hereby claim the date of priority under the International Convention of Japanese Patent Application No. P11-280075, filed September 30, 1999, as acknowledged in the Declaration of this application.

A certified copy of said Japanese Patent Application is submitted herewith.

Respectfully submitted,

Takashi YUMIBA et al.

By _____
Nils E. Pedersen
Registration No. 33,145
Attorney for Applicants

NEP/tf
Washington, D.C. 20006
Telephone (202) 721-8200
September 26, 2000

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９９年 ９月３０日

出 願 番 号
Application Number: 平成１１年特許願第２８００７５号

出 願 人
Applicant (s): 松下電器産業株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年 ７月２１日

特 許 庁 長 官
Commissioner,
Patent Office 及 川 耕 造

出証番号 出証特２０００－３０５６１８９

【書類名】　特許願

【整理番号】　2032410354

【提出日】　平成11年 9月30日

【あて先】　特許庁長官　殿

【国際特許分類】　G11B 19/00

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　弓場　隆司

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　石原　秀志

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　福島　能久

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　館林　誠

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　横田　薫

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100077931

【弁理士】

【氏名又は名称】　前田　弘

【選任した代理人】

【識別番号】　100094134

【弁理士】

【氏名又は名称】　小山　廣毅

【手数料の表示】

【予納台帳番号】　014409

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9601026

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報記録媒体、情報再生方法および情報再生装置

【特許請求の範囲】

【請求項１】　コンテンツ情報が記録された情報記録媒体であって、

リードイン領域と、

データ記録領域とを有し、

前記リードイン領域には第１の暗号化鍵情報が記録され、

前記データ記録領域には少なくとも第２の暗号化鍵情報と前記コンテンツ情報とが記録され、

前記データ記録領域に記録された前記コンテンツ情報はその一部がスクランブルされて記録されており、

このスクランブルされて記録されたコンテンツ情報は、前記第２の暗号化鍵情報を前記コンテンツ情報のうちスクランブルされていない部分を用いて変換することによって得られるスクランブル鍵情報を用いて、スクランブルされている

ことを特徴とする情報記録媒体。

【請求項２】　請求項１に記載の情報記録媒体において、

前記データ記録領域は複数のセクタに分割されており、

前記セクタのそれぞれは、セクタを識別する情報を記録するセクタヘッダ領域と、前記コンテンツ情報を記録するメインデータ領域とを有し、

前記セクタヘッダ領域には前記第２の暗号化鍵情報が記録され、

前記メインデータ領域に記録された前記コンテンツ情報はその一部がスクランブルされて記録されており、

このスクランブルされて記録されたコンテンツ情報は、前記第２の暗号化鍵情報をセクタ毎の前記コンテンツ情報のうちスクランブルされていない部分を用いて変換することによって得られるスクランブル鍵情報を用いて、スクランブルされている

ことを特徴とする情報記録媒体。

【請求項３】　請求項１又は２に記載の情報記録媒体において、

前記スクランブル鍵情報を作成する際に用いられる前記コンテンツ情報のうち

スクランブルされていない部分には、少なくともコピー制御情報を含む
ことを特徴とする情報記録媒体。

【請求項４】　請求項２に記載の情報記録媒体において、
前記スクランブル鍵情報を作成する際に用いられる前記コンテンツ情報のうちスクランブルされていない部分には、少なくとも、
コピー制御情報と、
セクタ毎に変化するコンテンツ情報の一部とを含む
ことを特徴とする情報記録媒体。

【請求項５】　請求項２に記載の情報記録媒体において、
前記セクタヘッダに記録される前記第２の暗号化鍵情報は、
前記リードイン領域に記録される前記第１の暗号化鍵情報を用いて暗号化されたものである
ことを特徴とする情報記録媒体。

【請求項６】　リードイン領域とデータ記録領域とを備え、前記リードイン領域には第１の暗号化鍵情報が記録され、前記データ記録領域には少なくとも第２の暗号化鍵情報とコンテンツ情報とが記録され、前記コンテンツ情報はその一部がスクランブルされて記録されている情報記録媒体を再生する情報再生方法であって、
前記リードイン領域に記録された前記第１の暗号化鍵情報を復号し、
この復号結果を用いて前記データ記録領域に記録された前記第２の暗号化鍵情報を復号し、
この復号結果を前記データ記録領域に記録された前記コンテンツ情報のうちスクランブルされていない部分を用いて変換し、
この変換結果を用いてスクランブルされて記録されたコンテンツ情報をデスクランブルする
ことを特徴とする情報再生方法。

【請求項７】　リードイン領域とデータ記録領域とを備え、前記リードイン領域には第１の暗号化鍵情報が記録され、前記データ記録領域には少なくとも第２の暗号化鍵情報とコンテンツ情報とが記録され、前記コンテンツ情報はその一

部がスクランブルされて記録されている情報記録媒体を再生する情報再生装置であって、

前記情報記録媒体のリードイン領域に記録された前記第１の暗号化鍵情報を復号する第１の鍵情報復号手段と、

前記データ記録領域に記録された前記第２の暗号化鍵情報を復号する第２の鍵情報復号手段と、

前記第２の鍵情報復号手段の出力を前記データ記録領域に記録された前記コンテンツ情報のうちスクランブルされていない部分を用いて変換する鍵情報変換手段と、

前記スクランブルされて記録されたコンテンツ情報を前記鍵情報変換手段の出力によりデスクランブルするデスクランブル手段と

を備えたことを特徴とする情報再生装置。

【請求項８】　請求項７に記載の情報再生装置において、

前記コンテンツ情報のうちスクランブルされていない部分には、少なくともコピー制御情報を含む

ことを特徴とする情報再生装置。

【請求項９】　請求項７に記載の情報再生装置において、

前記第２の鍵情報復号手段は、

前記第１の鍵情報復号手段の出力を用いて、前記第２の暗号化鍵情報を復号する

ことを特徴とする情報再生装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、映像情報や音声情報等を記録する情報記録媒体と、情報記録媒体に記録された情報を再生する情報再生装置に関するものである。

【０００２】

【従来の技術】

近年、音声情報の記録媒体としてコンパクトテープやアナログレコードなどの

アナログ信号で記録する記録媒体から、ＣＤ（Compact Disc）やＭＤ（Mini Disc）などのディジタル信号で記録する記録媒体が主流になってきている。また、映像信号の記録媒体もＭＰＥＧ（moving picture coding experts group）１と呼ばれる圧縮方式で圧縮された映像信号をＣＤに記録するVideo-CD、さらには４．７ＧＢの大容量を有する光ディスクにＭＰＥＧ２と呼ばれる高品位な圧縮方式による圧縮映像信号を記録するＤＶＤ（Digital Video Disc）などのディジタル記録媒体が開発され、映像・音声の記録媒体として商品化されている。

【０００３】

従来の情報再生装置の構成について簡単に説明する。図４は従来の情報再生装置の構成図である。図４において、４００は光ディスクから読み出したデータを誤り訂正処理や伸長処理を施して所望の映像信号や音声信号を出力する情報再生装置全体を示している。２０１は光ディスク、２０２は光ディスク２０１を後述するサーボ制御手段２１１により回転させるスピンドルモータ、２０３はレーザーを駆動して光ディスク２０１を照射し反射光を受光する光学ヘッド、２０４は光学ヘッド２０３からの出力信号を増幅するヘッドアンプ、２０５はＡＧＣ（auto gain control）、イコライズ、データライス、ＰＬＬ（phase-locked-loop）の機能を有するアナログ処理部、２０６は再生データを復調し、誤り訂正処理などを行う光ディスクコントローラ、２０７は光ディスクコントローラ２０６でエラー訂正に用いる誤り訂正用メモリ、２０９は圧縮されている映像・音声データに対して伸長処理を施し、音声信号と映像信号として出力するＡＶデコーダ（オーディオ・ビデオデコード手段）、２１０は映像・音声データの伸長処理に用いられるＡＶ信号処理用メモリ（伸張用バッファメモリ）、２１１はフォーカス、トラッキングなどのサーボ制御を行うサーボ制御手段である。４１２はＣＰＵであり、ＣＰＵバス２１３を介してアナログ処理部２０５、光ディスクコントローラ２０６、ＡＶデコーダ２０９、サーボ制御手段２１１を制御し、装置全体の動作を制御する。

【０００４】

従来の情報再生装置の動作について、図４を用いて簡単に説明する。ＣＰＵ４１２は所定のシーケンスで、光ディスク２０１からデータを読み出し、エラー訂

正が施されたデータを誤り訂正用メモリ２０７に格納されるように制御する。この時、ＣＰＵ４１２は誤り訂正用メモリ２０７に格納されたデータのうち、制御情報やデータの識別情報を読み出し、サーボ制御手段２１１を制御したり、ＡＶデコーダ２０９の制御を行ったりして、ビデオデータやオーディオデータの再生を行っている。

【０００５】

一方、パーソナルコンピュータ（以下ＰＣ）の高性能化やハードディスクの大容量化に伴い、ＰＣのアプリケーションプログラムも大容量化が進んでいる。ＤＶＤはその大容量の特徴を活かし映像・音声の記録媒体だけでなく、ＰＣのアプリケーションソフトウェア等の頒布媒体としても活用されており、ＰＣの周辺装置としてのＤＶＤドライブの普及が急激に進んでいる。さらに、ＰＣ用としてＭＰＥＧの伸長機能を備えたＡＶデコーダカードや、ＰＣのメインプロセッサのソフトウェア処理によりＭＥＰＧ伸長機能を行うプログラムなども商品化されている。

【０００６】

しかしながら、ＤＶＤドライブとＡＶデコーダカードを用いてＰＣでＤＶＤの映像・音声のデータを再生するシステムでは、これらの装置間は一般的なコンピュータバスの通信路により接続されていることから、通信路を介して伝送されるデータの不正コピーや、データを改竄されて頒布されるなどの行為が行われ、著作権者の権利を保護することが極めて困難となるという課題がある。

【０００７】

この課題に対応するために、著作権を有するデータを暗号化して記録することが提案されている。特開平７－２４９２６４号公報の図３に開示されたＣＤ－ＲＯＭでは、暗号化されたデータセクタとは異なるセクタのメインデータ領域に暗号鍵を記録する方式が提案されている。本従来例では、記録時に暗号化されたデータとその暗号鍵をＣＤ－ＲＯＭに記録し、再生時にはパーソナルコンピュータから再生装置に対して暗号鍵の読み出し命令を行った後に暗号化データを読み出して、先に読み出した暗号鍵を用いて復号することにより、データ再生を実現するというものである。

【０００８】

【発明が解決しようとする課題】

しかしながら、特開平７－２４９２６４号公報に開示された従来例では、暗号鍵が一般的な読み出し命令（Readコマンド）によって読み出すことができるセクタのメインデータ領域に記録されているため、暗号鍵を一般のパーソナルコンピュータから容易に読み出すことができる。

【０００９】

従って、暗号鍵と暗号化データをユーザが読み出すことができるために、暗号の解読を行われる危険性が高いという課題があるとともに、暗号鍵と暗号化データを例えばハードディスクにコピーされて不正な複製を作成される可能性があるという課題がある。

【００１０】

また、セクタのメインデータ領域全てを暗号化して記録されているために、ＤＶＤプレイヤの様に、セクタのメインデータ中に含まれる、コンテンツの識別情報やコンテンツのコピー制御情報等が含まれるコンテンツ制御情報を、ＤＶＤプレイヤの制御のためにＣＰＵで読み込もうとすると、一度暗号化されたデータを復号してからでないと正しい情報を得ることはできない。

【００１１】

上記した課題に対して、コンテンツ制御情報が含まれる領域を平文のまま記録してしまうと、コピー制御情報が不正に改竄された場合、不正な再生が行われることになる。

【００１２】

本発明は上記問題点に鑑み、デスクランブル処理に用いる鍵情報を容易に読み出されないことを実現するためのデータ構造を有する情報記録媒体を提供し、かつプレイヤにおいて、プレイヤを制御するＣＰＵが容易にコピー制御情報等を読み込み、プレイヤの制御を行え、かつコピー制御情報等が不正に改竄されても、正常に再生できない情報記録媒体、情報再生方法および情報再生装置を提供することを目的とする。

【００１３】

【課題を解決するための手段】

前記課題を解決するため、請求項１の発明が講じた手段は、コンテンツ情報が記録された情報記録媒体であって、リードイン領域と、データ記録領域とを有し、前記リードイン領域には第１の暗号化鍵情報が記録され、前記データ記録領域には少なくとも第２の暗号化鍵情報と前記コンテンツ情報とが記録され、前記データ記録領域に記録された前記コンテンツ情報はその一部がスクランブルされて記録されており、このスクランブルされて記録されたコンテンツ情報は、前記第２の暗号化鍵情報を前記コンテンツ情報のうちスクランブルされていない部分を用いて変換することによって得られるスクランブル鍵情報を用いて、スクランブルされているものである。

【００１４】

また、請求項２の発明は、請求項１に記載の情報記録媒体において、前記データ記録領域は複数のセクタに分割されており、前記セクタのそれぞれは、セクタを識別する情報を記録するセクタヘッダ領域と、前記コンテンツ情報を記録するメインデータ領域とを有し、前記セクタヘッダ領域には前記第２の暗号化鍵情報が記録され、前記メインデータ領域に記録された前記コンテンツ情報はその一部がスクランブルされて記録されており、このスクランブルされて記録されたコンテンツ情報は、前記第２の暗号化鍵情報をセクタ毎の前記コンテンツ情報のうちスクランブルされていない部分を用いて変換することによって得られるスクランブル鍵情報を用いて、スクランブルされているものである。

【００１５】

さらに、請求項３の発明は、請求項１又は２に記載の情報記録媒体において、前記スクランブル鍵情報を作成する際に用いられるスクランブルされていないコンテンツ情報の一部には、少なくともコピー制御情報を含むものである。

【００１６】

また、請求項４の発明は、請求項２に記載の情報記録媒体において、前記スクランブル鍵情報を作成する際に用いられる前記コンテンツ情報のうちスクランブルされていない部分には、少なくとも、コピー制御情報と、セクタ毎に変化するコンテンツ情報の一部とを含むものである。

【００１７】

また、請求項５の発明では、請求項２に記載の情報記録媒体において、前記セクタヘッダに記録される前記第２の暗号化鍵情報は、前記リードイン領域に記録される前記第１の暗号化鍵情報を用いて暗号化されたものである。

【００１８】

また、請求項６の発明は、リードイン領域とデータ記録領域とを備え、前記リードイン領域には第１の暗号化鍵情報が記録され、前記データ記録領域には少なくとも第２の暗号化鍵情報とコンテンツ情報とが記録され、前記コンテンツ情報はその一部がスクランブルされて記録されている情報記録媒体を再生する情報再生方法であって、前記リードイン領域に記録された前記第１の暗号化鍵情報を復号し、この復号結果を用いて前記データ記録領域に記録された前記第２の暗号化鍵情報を復号し、この復号結果を前記データ記録領域に記録された前記コンテンツ情報のうちスクランブルされていない部分を用いて変換し、この変換結果を用いてスクランブルされて記録されたコンテンツ情報をデスクランブルするものである。

【００１９】

また、請求項７の発明は、リードイン領域とデータ記録領域とを備え、前記リードイン領域には第１の暗号化鍵情報が記録され、前記データ記録領域には少なくとも第２の暗号化鍵情報とコンテンツ情報とが記録され、前記コンテンツ情報はその一部がスクランブルされて記録されている情報記録媒体を再生する情報再生装置であって、前記情報記録媒体のリードイン領域に記録された前記第１の暗号化鍵情報を復号する第１の鍵情報復号手段と、前記データ記録領域に記録された前記第２の暗号化鍵情報を復号する第２の鍵情報復号手段と、前記第２の鍵情報復号手段の出力を前記データ記録領域に記録された前記コンテンツ情報のうちスクランブルされていない部分を用いて変換する鍵情報変換手段と、前記スクランブルされて記録されたコンテンツ情報を前記鍵情報変換手段の出力によりデスクランブルするデスクランブル手段とを備えたものである。

【００２０】

また、請求項８の発明は、請求項７に記載の情報再生装置において、前記コン

テンツ情報のうちスクランブルされていない部分には、少なくともコピー制御情報を含むものである。

【００２１】

また、請求項９の発明は、請求項７に記載の情報再生装置において、前記第２の鍵情報復号手段は、前記第１の鍵情報復号手段の出力を用いて、前記第２の暗号化鍵情報を復号するものである。

【００２２】

本発明によると、情報記録媒体のデータ記録領域にスクランブル処理を施して記録する際に、情報記録媒体に記録された鍵情報をコピー制御情報やデータの一部を用いて変換してスクランブル用鍵情報として生成するので、コピー制御情報にスクランブル処理を施さなくても、不正に改竄された場合にはスクランブル鍵情報が異なるものとなり、正常な再生ができなくなる。またデータの一部を用いることにより、セクタ毎にスクランブル用鍵情報が異なるので、不正な攻撃に対して強度が強くなる。

【００２３】

【発明の実施の形態】

以下、本発明の一実施形態に係る情報記録媒体及び情報再生装置に関して、図面を参照しながら説明する。以下、情報記録媒体として光ディスク（ＤＶＤ）を例に取り説明する。

【００２４】

図１は本実施形態における情報記録媒体のデータ構造を示す説明図である。図１（ａ）はディスク全体の情報記録領域の構造を示しており、制御情報が記録されるリードイン領域１００と、コンテンツ制御情報とコンテンツデータからなるコンテンツ情報が記録されるデータ記録領域１０１、リードアウト領域１０２とから構成されている。

【００２５】

リードイン領域１００には、情報再生装置が光ディスクを再生するために必要とする情報が記録されるコントロールデータ領域１１０が含まれており、コントロールデータ領域は、図１（ｂ）で示すように物理情報セクタ１１１やスクラン

ブル情報セクタ１１２等を含んでいる。物理情報セクタ１１１にはディスク径、ディスク構造、記録密度などのディスクの物理情報が記録されており、スクランブル情報セクタ１１２には第１の鍵情報に暗号を施した第１の暗号化鍵情報が記録されている。

【００２６】

データ記録領域には、圧縮された映画や音楽等のコンテンツ情報がファイルとして記録されている。図１（ａ）に示すように、著作権を保護すべきコンテンツはスクランブルされてスクランブルファイル１２０として記録され、著作権がフリーなコンテンツはスクランブルされずに、非スクランブルファイル１３０として記録されている。

【００２７】

データ記録領域はセクタと呼ばれる単位で区切られている。図１（ｃ）及び（ｄ）に示すように、スクランブルファイル１２０はスクランブルセクタ、非スクランブルファイル１３０は非スクランブルセクタを有している。図１（ｅ）及び（ｆ）に示すように、スクランブルセクタ、非スクランブルセクタは、セクタを識別するためのアドレス情報等が記録される１２バイトのセクタヘッダ領域１２１、１３１と、コンテンツ情報が記録される２０４８バイトのメインデータ領域１２２、１３２を有している。スクランブルセクタのセクタヘッダ領域１２１には、前述のアドレス情報に加え、スクランブルフラグや第２の鍵情報に暗号を施した第２の暗号化鍵情報１２３等が記録されている。非スクランブルセクタのセクタヘッダ領域１３１においては、スクランブルセクタのセクタヘッダ領域１２１で第２の暗号化鍵情報１２３が格納される領域に相当する領域はリザーブ状態とされ、この領域全てに“０”が記録される。

【００２８】

セクタヘッダ領域１２１、１３１に記録されるスクランブルフラグはそのセクタのメインデータ領域の所定領域がスクランブルされているか否かを示すフラグであり、スクランブルデータが記録されているスクランブルセクタの場合にはスクランブルフラグは“１”、非スクランブルセクタの場合にはスクランブルフラグは“０”が記録される。

【００２９】

セクタヘッダ領域に記録される第２の暗号化鍵情報１２３は、リードイン領域１００のスクランブル情報セクタ１１２に記録されている第１の暗号化鍵情報を復号した結果を鍵として復号処理され、復号された第２の鍵情報はメインデータのデスクランブル処理に用いられる情報となる。

【００３０】

また、図１（ｅ）に示すように、スクランブルセクタのメインデータ領域１２２は、メインデータ領域の全てをスクランブルして記録するものではなく、図１（ｇ）に示すようにコンテンツ制御情報１２４が含まれる領域やコンテンツデータの一部を除いてスクランブルされている。コピー制御情報１２６には、コンテンツのコピー制限回数や再生時のダウンサンプリング制御等の情報が記載されている。このスクランブルされたコンテンツデータは、第２の暗号化鍵情報を、コンテンツ制御情報１２４に含まれるコピー制御情報及び圧縮されたコンテンツの一部（図１（ｇ）の参照データ１２７）を用いて変換して得られるスクランブル鍵情報により、所定領域のデータをスクランブルされて記録されている。

【００３１】

以上の様に、構成された情報記録媒体を用いた情報再生装置の実施の形態について、図を用いて説明する。

【００３２】

図２は、本実施形態の情報再生装置の全体を示す構成図である。２００は光ディスク２０１から読み出したデータをデスクランブル処理や伸長処理を施して所望の映像信号や音声信号を出力する情報再生装置全体を示している。図４に示した従来例における構成要素と同じものには同じ番号を付与している。

【００３３】

２０１は図１で示したデータ構造を持つ光ディスク、２０２は光ディスク２０１を後述するサーボ制御手段２１１により回転させるスピンドルモータ、２０３はレーザーを駆動して光ディスク２０１を照射し反射光を受光する光学ヘッド、２０４は光学ヘッド２０３からの出力信号を増幅するヘッドアンプ、２０５はＡＧＣ、イコライズ、データライス、ＰＬＬの機能を有するアナログ処理部、２０

６は再生データを復調し、誤り訂正処理などを行う光ディスクコントローラ、２０７は光ディスクコントローラ２０６でエラー訂正に用いる誤り訂正用メモリ、２０８はスクランブルされて記録されている情報にデスクランブル処理を施すデスクランブル回路、２０９は圧縮されている映像・音声データに対して伸長処理を施し、音声信号と映像信号として出力するＡＶデコーダ（オーディオ・ビデオデコード手段）、２１０は映像・音声データの伸長処理に用いられるＡＶ信号処理用メモリ、２１１はフォーカス、トラッキングなどのサーボ制御を行うサーボ制御手段である。２１２はＣＰＵであり、プログラムＲＯＭ（図示せず）に格納されたプログラムに従って、ＣＰＵバス２１３を介してアナログ処理部２０５、光ディスクコントローラ２０６、デスクランブル回路２０８、ＡＶデコーダ２０９、サーボ制御手段２１１を制御し、装置全体の動作を制御する。

【００３４】

デスクランブル回路２０８はリードイン領域１００のスクランブル情報セクタ１１２に記録されている第１の暗号化鍵情報を入力し、第１の暗号化鍵情報を復号するとともに、図１（ｃ）で示した構造を持つセクタデータを入力し、第２の暗号化鍵情報の復号処理及びメインデータのデスクランブル処理を実施するものである。

【００３５】

デスクランブル回路２０８について説明する。図３はデスクランブル回路２０８の全体構成を示す構成図である。３０１はＣＰＵバス２１３を経由してＣＰＵ２１２から設定される復号モード設定情報に応じて、入力されるデータの内部での出力先を選択する第１の信号選択手段、３０２は第１の暗号化鍵情報の復号に用いる固定鍵を格納する固定鍵情報格納手段、３０３は第１の信号選択手段３０１から出力されるセクタデータを入力して、セクタデータのセクタ内の位置に応じて、つまりセクタデータのデータ数をカウントしたカウント値に応じて、出力先を選択する第２の信号選択手段である。

【００３６】

また３０４は第１の鍵情報復号手段であり、第１の信号選択３０１から出力されるリードイン領域のスクランブル情報セクタ１１２の第１の暗号化鍵情報に対

して固定鍵情報格納手段３０２から出力される固定鍵情報を用いて復号処理を行い、復号された第１の鍵情報を出力するものである。３０５は第２の鍵情報復号手段であり、第２の信号選択手段３０３から出力される第２の暗号化鍵情報を入力し、第１の鍵情報復号手段３０４から出力される、復号された第１の鍵情報を用いて復号処理を行い、復号された第２の鍵情報を出力するものである。

【００３７】

さらに、３１０は、第２の鍵情報復号手段３０５から出力される、復号された第２の鍵情報を、第２の信号選択手段から出力されるコピー制御情報と参照データとを用いて変換し、デスクランブル用鍵情報を出力する鍵情報変換手段であり、復号された第２の鍵情報をコピー制御情報を用いて変換する第１の鍵変換手段３１１と、第１の鍵変換手段３１１の出力を参照データを用いて変換する第２の変換手段３１２とを備えている。

【００３８】

３０６は第２の信号選択手段３０３から出力されるメインデータを入力し、鍵情報変換手段３１０から出力されるデスクランブル用鍵情報を用いてデータのデスクランブル処理を施すデータデスクランブル手段、３０７はデータデスクランブル手段３１０の出力及び第２の信号選択手段３０３の出力のうち、いずれか一つを選択して出力する第３の信号選択手段である。

【００３９】

以上の様に構成された、本実施形態の情報再生装置の動作について、図１～３を参照して説明する。

【００４０】

情報再生装置（光ディスク再生装置）２００は電源投入時にディスクが挿入されている場合、又は新たにディスクが挿入された場合には、リードイン領域１００のスクランブル情報セクタ１１２に記録されている第１の暗号化鍵情報の復号処理を行う。ＣＰＵ２１２はサーボ制御手段２１１を制御して光学ヘッド２０３からリードイン領域１００のスクランブル情報セクタ１１２の情報を読み出すよう制御する。

【００４１】

読み出された信号には、ヘッドアンプ２０４、アナログ処理部２０５及び光ディスクコントローラ２０６により、順次増幅、復調処理及びエラー訂正が施される。

【００４２】

また、ＣＰＵ２１２はデスクランブル回路２０８に対して復号モード設定情報として第１の暗号化鍵情報を復号するモードを設定し、光ディスクコントローラ２０６からエラー訂正処理後のスクランブル情報セクタ１１２をデスクランブル回路２０８に転送するよう制御する。

【００４３】

デスクランブル回路２０８では、第１の鍵情報復号モードが設定されることから、入力されたスクランブル情報セクタ１１２のデータは第１の信号選択手段３０１により第１の鍵情報復号手段３０４に転送され、第１の鍵情報復号手段３０４により固定鍵情報格納手段３０２から出力される固定鍵情報を用いて復号処理が施される。なお、この第１の鍵情報を復号するモードではデスクランブル回路２０８からはデータは出力されない。

【００４４】

続いて装置使用者の操作等に応じてファイルが選択され、映像や音声を再生する動作を説明する。

【００４５】

ＣＰＵ２１２はサーボ制御手段２１１や光学ヘッド２０３、アナログ処理部２０５、光ディスクコントローラ２０６を制御して光ディスク２０１から所望の情報を読み出し、エラー訂正後のデータを誤り訂正用メモリ２０７に格納する。また、ＣＰＵ２１２はデスクランブル回路２０８に対してデータのデスクランブルモードを設定するとともに、ＡＶデコーダ２０９に必要な情報を設定した後に、エラー訂正後のデータを誤り訂正用メモリ２０７からデスクランブル回路２０８に転送する。

【００４６】

デスクランブル回路２０８では、データ復号モード設定情報としてデータのデスクランブルモードに設定されることから、第１の信号選択手段３０１により、

入力されるセクタデータは、第２の信号選択手段３０３に転送される。第２の信号選択手段３０３では、入力されるデータ数をカウントし、カウント値が、セクタヘッダ領域の第２の暗号化鍵情報の位置を示す値の場合には第２の鍵情報復号手段３０５に、コピー制御情報が含まれるデータ位置を示す値の場合には第１の鍵変換手段３１１に、参照データの位置を示す値の場合には第２の鍵変換手段３１２に、メインデータの位置を示す値の場合にはデータデスクランブル手段３０６及び第３の信号選択手段３０７にそれぞれ出力するように、入力データを割り振る。

【００４７】

第２の鍵情報復号手段３０５に入力された暗号化された第２の暗号化鍵情報は、第１の鍵情報復号手段１０５から出力される復号された第１の暗号化鍵情報を鍵として用いて復号される。

【００４８】

そして復号された第２の鍵情報は、メインデータに含まれるコピー制御情報を用いて第１の鍵変換手段３１１で変換され、さらに第１の鍵変換手段３１１の出力は、メインデータに含まれる参照データにより第２の鍵変換手段３１２で変換され、デスクランブル用鍵情報が出力される。

【００４９】

データデスクランブル手段３０６に入力されたメインデータは鍵情報変換手段３１０から出力されるデスクランブル用鍵情報を用いてデスクランブル処理が施され第３の信号選択手段３０７に出力される。

【００５０】

第３の信号選択手段３０７は、第２の信号選択手段３０３により選択されたスクランブルフラグを入力し、かつ内部でセクタデータのデータ数をカウントし、この両者の値に応じて選択信号を出力する。この選択信号によって、スクランブルフラグが“１”でかつ、セクタのデータ数のカウント値が非スクランブル領域を示した場合は、デスクランブル処理を施されていないメインデータが第３の信号選択手段３０７から出力され、セクタのデータ数のカウント値がスクランブル領域を示した場合、データデスクランブル手段３０６の出力が第３の信号選択手

段３０７から出力される。

【００５１】

スクランブルフラグが“０”の場合には、セクタデータ数カウント値に関わらず、デスクランブル処理を施されていないメインデータが第３の信号選択手段３０７から出力される。

【００５２】

このようにスクランブルフラグに応じて、デスクランブル処理が施され、デスクランブル回路２０８から出力されたメインデータは、ＡＶデコーダ２０９に入力される。ＡＶデコーダ２０９は、多重化されたオーディオとビデオの圧縮データを分離して、それぞれに伸長処理を施して、映像信号、音声信号として出力する。

【００５３】

このように本発明によると、以下の様な効果がある。

【００５４】

まず、コピー回数制限や再生時のダウンサンプリング制御などのコンテンツ制御情報１２４を、情報再生装置（ＤＶＤプレイヤ）のシステムコントロール手段（図２のＣＰＵ２１２）が読み込んで、情報再生装置の制御を行う際に、コンテンツ制御情報はスクランブルされずに記録されているので、容易に参照することができる。

【００５５】

またコンテンツ制御情報１２４は、上記の観点からスクランブルされずに記録しているが、不正にコンテンツ制御情報１２４を改竄した場合、正しくデスクランブル鍵情報を生成することはできないので、不正な再生を防止することができる。

【００５６】

さらに、コピー制御情報１２４を用いて、第２の暗号化鍵情報からスクランブル鍵情報を得る際に、さらにセクタ単位で変化しやすいコンテンツデータを用いているので、コピー制御情報が前述のファイル単位に設定され、かつ第２の暗号化鍵情報も同様にファイル単位で設定されたとしても、スクランブル鍵情報がセ

クタ毎に変わるので、スクランブルによるコンテンツの保護強度を高くすることができる。

【００５７】

なお、本実施形態では、情報記録媒体として光ディスクを例として用いたが、磁気ディスク等の他の情報記録媒体であってもよい。

【００５８】

【発明の効果】

以上のように本発明の情報記録媒体では、リードイン領域には第１の暗号化鍵情報が記録され、データ記録領域には第２の暗号化鍵情報と、データ及びその一部がスクランブルされたスクランブルデータとが記録され、このスクランブルデータは、第２の暗号化鍵情報からスクランブルされていないデータに含まれるコピー制御情報や参照データを用いて生成されたスクランブル鍵情報を用いてスクランブルされたデータである。従って、装置内の制御のためにスクランブルされずに記録されたコピー制御情報が不正に改竄された場合には、スクランブルする際に用いられたスクランブル鍵情報を得ることができなくなるため、このような不正な行為が行われた場合に正常な再生を防止することが容易にできる。

【００５９】

さらに、スクランブルされていないデータを参照データとしてスクランブル鍵情報の生成に用いているので、例えば、第２の暗号化鍵情報やコピー制御情報がファイル単位で設定されたとしてもスクランブル鍵情報はセクタ単位で変化するので、不正な攻撃に対しても強いという効果がある。

【図面の簡単な説明】

【図１】

本実施形態における情報記録媒体のデータ構造を示す説明図である。

【図２】

本実施形態の情報再生装置の全体を示す構成図である。

【図３】

図２の情報再生装置におけるデスクランブル回路の全体構成を示す構成図である。

【図４】

従来の情報再生装置の構成図である。

【符号の説明】

１００　リードイン領域

１０１　データ記録領域

１０２　リードアウト領域

１１０　コントロールデータ領域

１１１　物理情報セクタ

１１２　スクランブル情報セクタ（第１の暗号化鍵情報）

１２０　スクランブルファイル

１３０　非スクランブルファイル

１２１、１３１　セクタヘッダ領域

１２２、１３２　メインデータ領域

１２３　第２の暗号化鍵情報

１２４　コンテンツ制御情報

１２５　コンテンツデータ

１２６　コピー制御情報

１２７　参照データ

２００、４００　情報再生装置

２０１　光ディスク

２０２　スピンドルモータ

２０３　光学ヘッド

２０４　ヘッドアンプ

２０５　アナログ処理部

２０６　光ディスクコントローラ

２０７　誤り訂正用メモリ

２０８　デスクランブル回路

２０９　ＡＶデコーダ

２１０　ＡＶ信号処理用メモリ

２１１　サーボ制御手段

２１２、４１２　ＣＰＵ

２１３　ＣＰＵバス

３０１　第１の信号選択手段

３０２　固定鍵情報格納手段

３０３　第２の信号選択手段

３０４　第１の鍵情報復号手段

３０５　第２の鍵情報復号手段

３０６　データデスクランブル手段

３０７　第３の信号選択手段

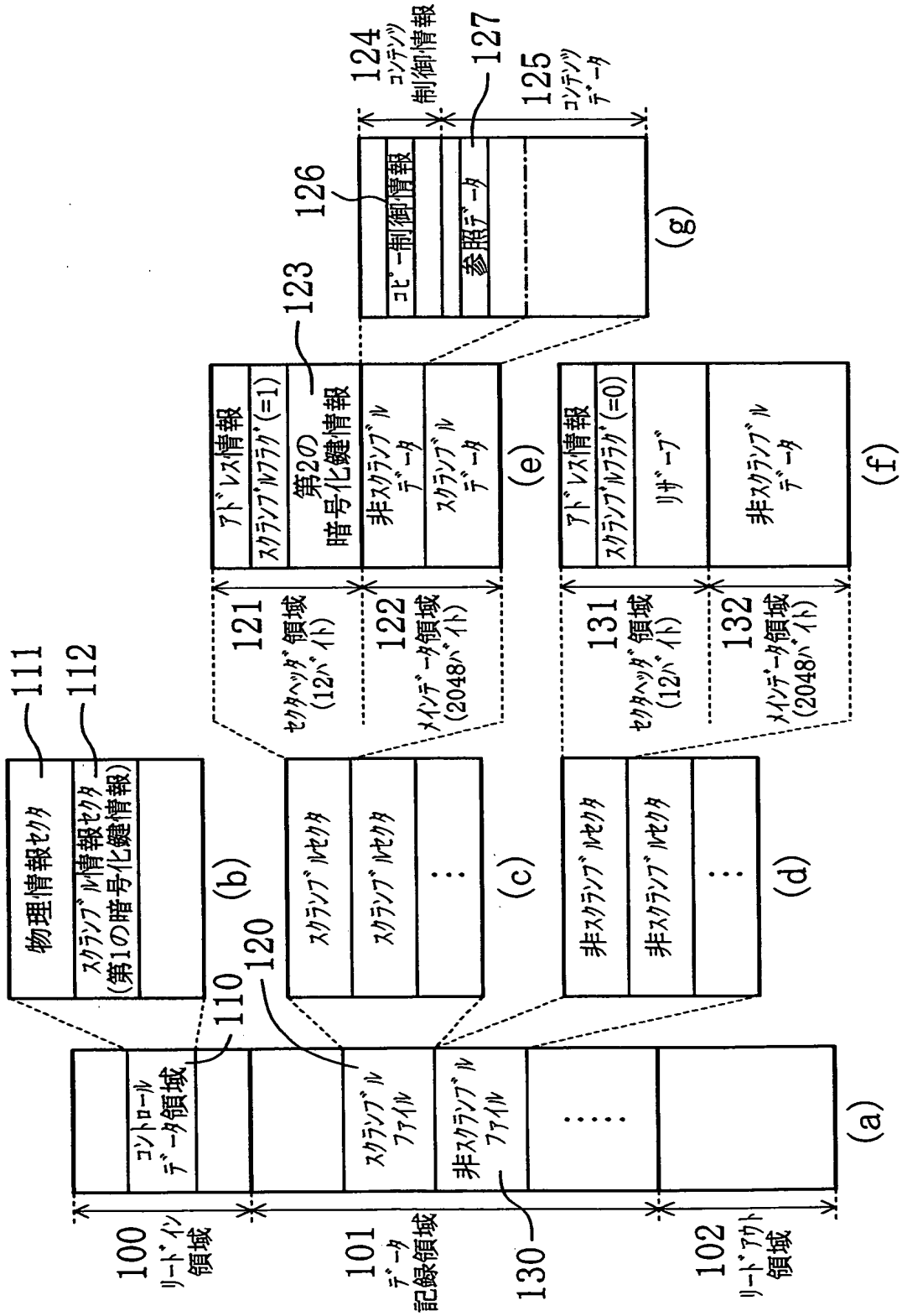
３１０　鍵情報変換手段

３１１　第１の鍵変換手段

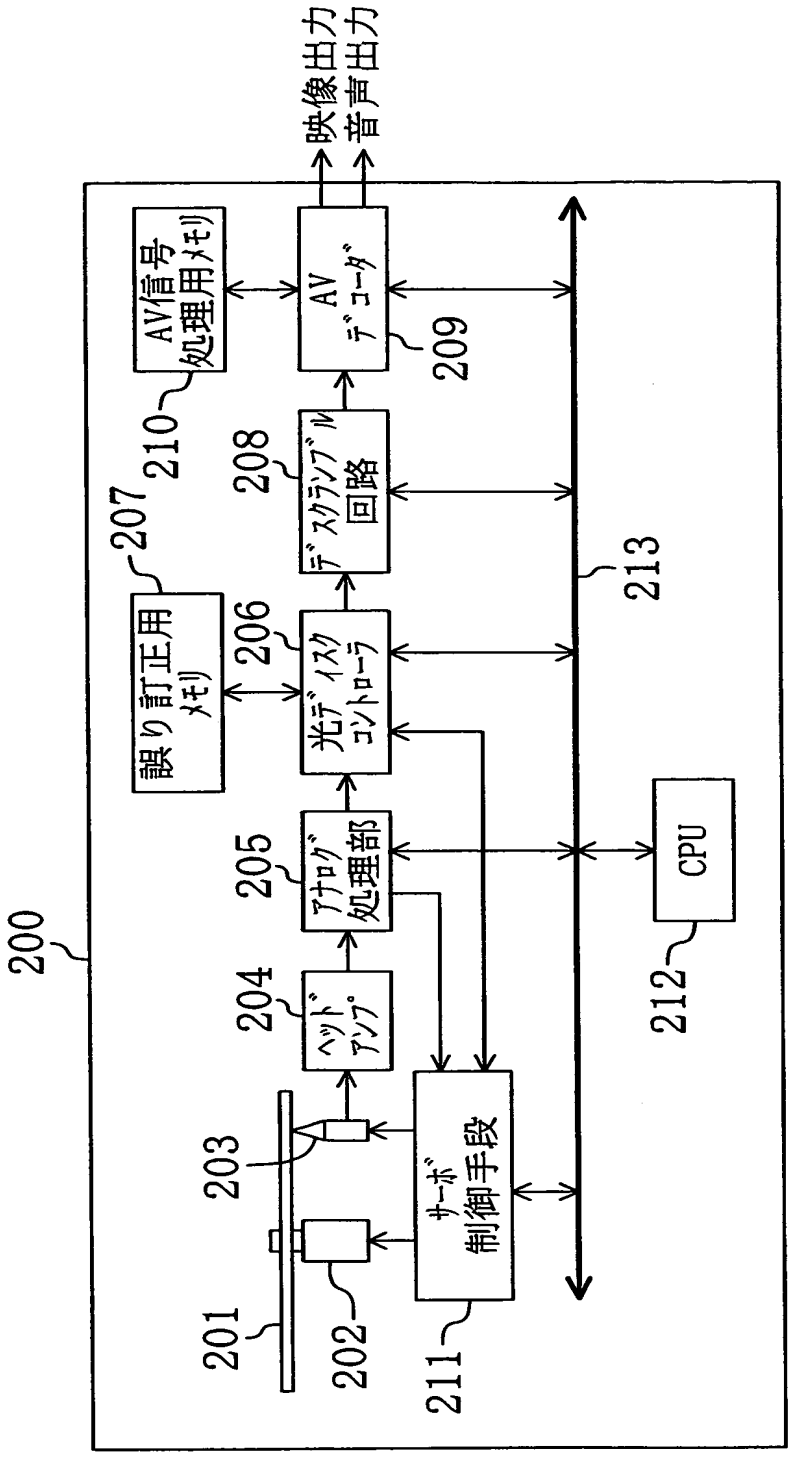
３１２　第２の鍵変換手段

【書類名】　図面

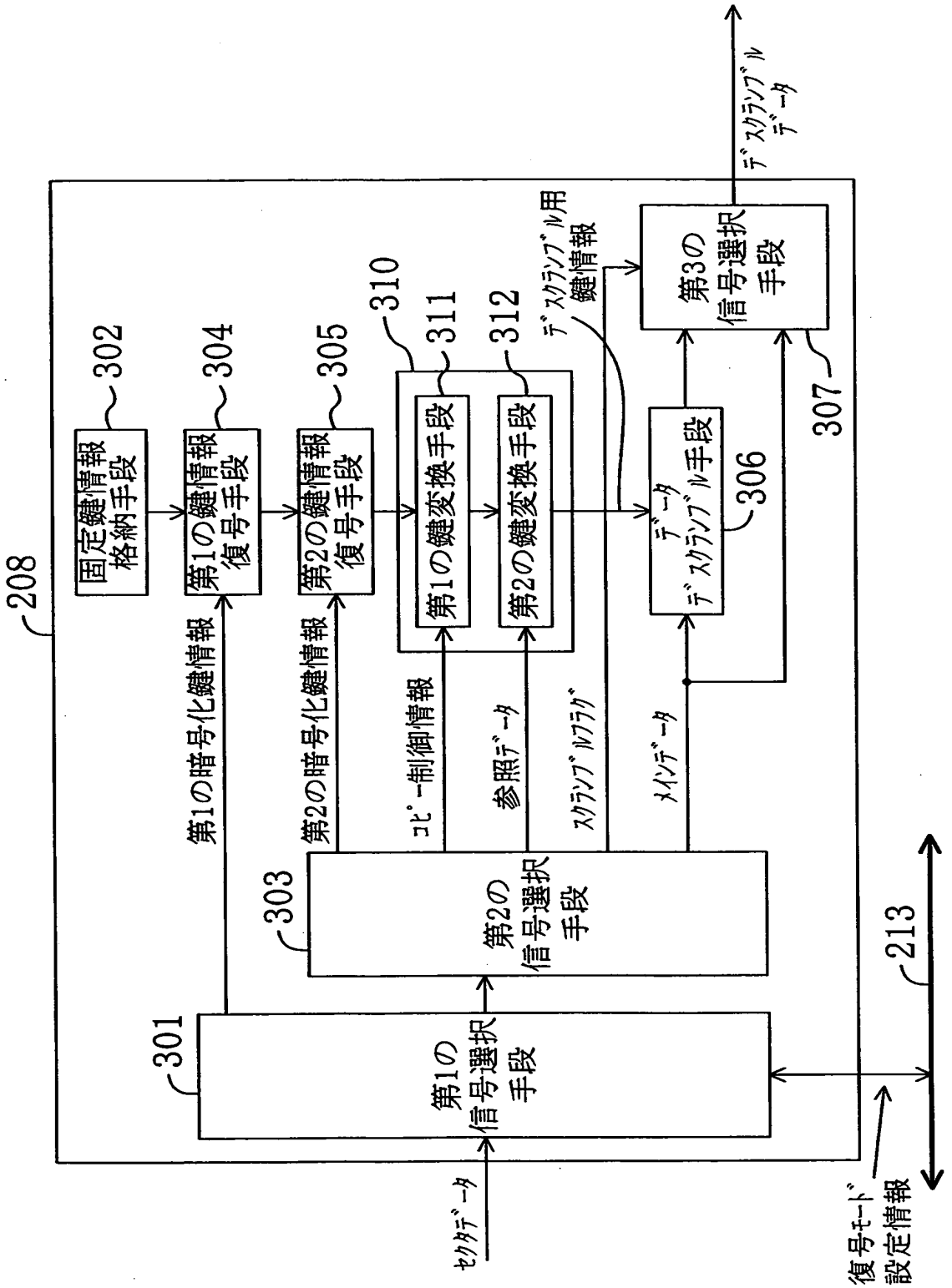
【図１】


100
リードイン領域
101
データ記録領域
102
リードアウト領域
130
(a)
コントロールデータ領域
110
スクランブルファイル
120
非スクランブルファイル
物理情報セクタ
111
スクランブル情報セクタ
(第1の暗号化鍵情報)
112
(b)
スクランブルセクタ
スクランブルセクタ
(c)
非スクランブルセクタ
非スクランブルセクタ
(d)
121
セクタヘッダ領域
(12バイト)
122
メインデータ領域
(2048バイト)
アドレス情報
スクランブルフラグ(=1)
123
第2の暗号化鍵情報
非スクランブルデータ
スクランブルデータ
(e)
131
セクタヘッダ領域
(12バイト)
132
メインデータ領域
(2048バイト)
アドレス情報
スクランブルフラグ(=0)
リザーブ
非スクランブルデータ
(f)
126
コピー制御情報
参照データ
127
124
コンテンツ制御情報
125
コンテンツデータ
(g)

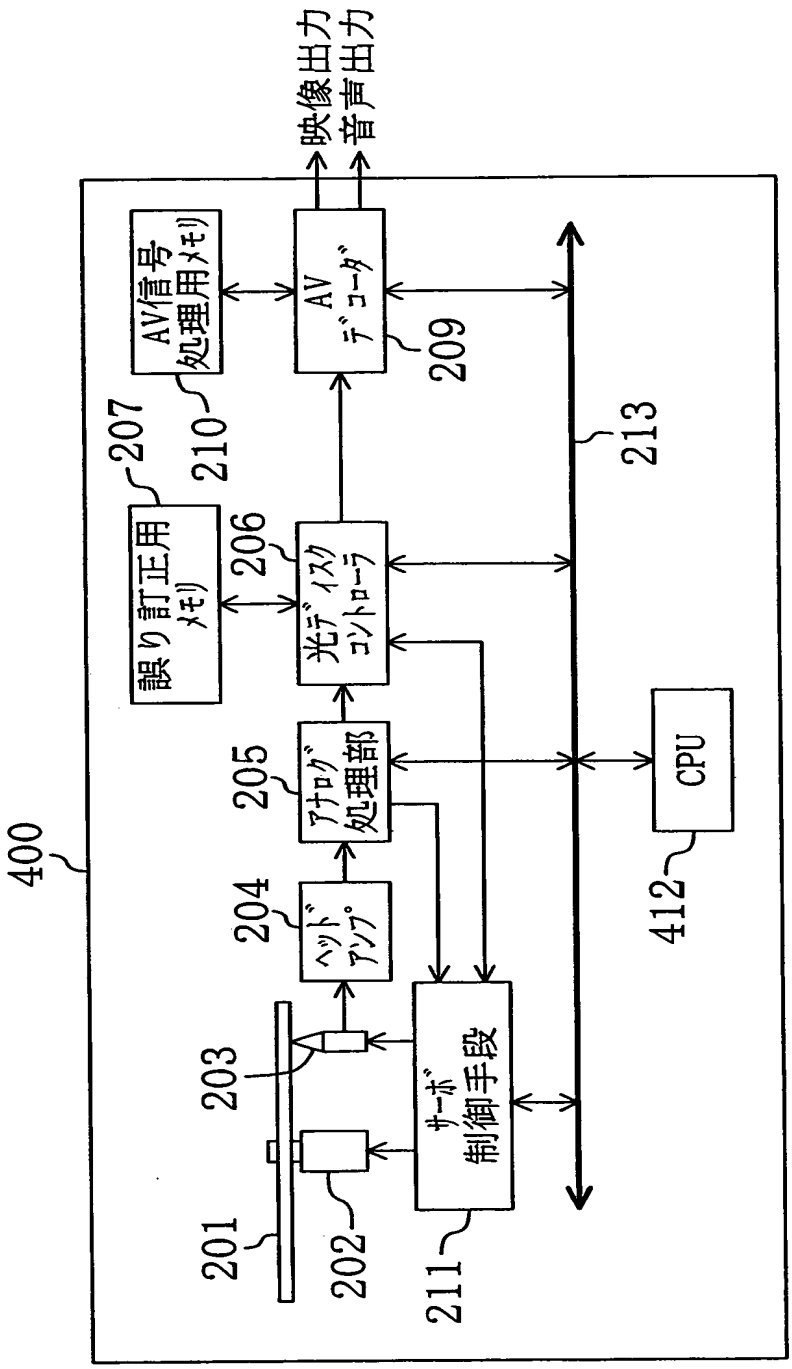
【図２】


映像出力
音声出力
AV信号処理用メモリ
AV デコーダ
209
210
208
デスクランブル回路
207
誤り訂正用メモリ
206
光ディスクコントローラ
213
205
アナログ処理部
CPU
200
204
ヘッドアンプ
212
203
サーボ制御手段
201
202
211

【図３】


208
固定鍵情報格納手段
302
第1の鍵情報復号手段
304
第2の鍵情報復号手段
305
310
311
312
第1の鍵変換手段
第2の鍵変換手段
データデスクランブル手段
306
第3の信号選択手段
307
デスクランブル用鍵情報
デスクランブルデータ
第1の暗号化鍵情報
第2の暗号化鍵情報
コピー制御情報
参照データ
スクランブルフラグ
メインデータ
303
第2の信号選択手段
301
第1の信号選択手段
213
セクタデータ
復号モード設定情報

【図４】


映像出力
音声出力
AV信号処理用メモリ
AVデコーダ
209
207
210
213
誤り訂正用メモリ
206
光ディスクコントローラ
205
アナログ処理部
CPU
400
204
ヘッドアンプ
412
203
サーボ制御手段
201
202
211

【書類名】　　要約書

【要約】

【課題】　コンテンツ情報内のコピー制御情報の不正な改竄に対処できるとともに、コピー制御情報を再生装置で容易に判別できる情報記録媒体を提供する。

【解決手段】　情報記録媒体は、リードイン領域とデータ記録領域とを備え、リードイン領域には第１の暗号化鍵情報が記録され、データ記録領域には第２の暗号化鍵情報とコンテンツ情報とが記録されている。コンテンツ情報は、その一部がスクランブル鍵情報を用いてスクランブルされて記録されている。スクランブル鍵情報は、コンテンツ情報のうちスクランブルされていない部分を用いて前記第２の暗号化鍵情報を変換して得られる。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
［変更理由］　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社